



ABB Doc Id:	Date	Lang.	Rev.	Page
1MRG023796	2016-10-24	English	A	1/4

TCP Predictability Vulnerability in Relion 650 series ABB-VU-PGGA-1MRG019772

Notice

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB.

ABB provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall ABB or any of its suppliers be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if ABB or its suppliers have been advised of the possibility of such damages.

This document and parts hereof must not be reproduced or copied without written permission from ABB, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

All rights to registrations and trademarks reside with their respective owners.

Copyright © 2016 ABB. All rights reserved.

Affected Products

Relion 650 series version 1.3.0.2 and earlier releases.

Summary

The operating system used by the device (VxWorks) has a weakness in the random number generator of the TCP implementation that may allow remote attackers to predict the correct TCP ISN (Initial Sequence Number) from previous values. This vulnerability affects the product versions listed above.

Additional Information can be found here:

- <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2001-0328>
- <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3963>

This vulnerability could be exploited remotely. Successful exploitation of this vulnerability may allow an attacker to spoof or disrupt TCP connections of the affected products.



ABB Doc Id: 1MRG023796	Date 2016-10-24	Lang. English	Rev. A	Page 2/4
---------------------------	--------------------	------------------	-----------	-------------

Severity rating

The CVSS score for this vulnerability is 5.8.. This assessment is based on the types of systems that are affected by the vulnerability, how difficult it is to exploit, and the effect that a successful attack exploiting the vulnerability could have.

CVSS Overall Score: 5.8

CVSS Vector: (AV:N/AC:M/Au:N/C:P/I:N/A:P)

CVSS Link:

[https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2015-3963&vector=\(AV:N/AC:M/Au:N/C:P/I:N/A:P\)](https://nvd.nist.gov/cvss/v2-calculator?name=CVE-2015-3963&vector=(AV:N/AC:M/Au:N/C:P/I:N/A:P))

Corrective Action or Resolution

ABB has investigated this vulnerability and have now released a maintenance release in order to provide adequate protection to customers.

Affected product version	Version where issue is mitigated
650 1.3	650 1.3.0.3

Prior to version Relion 650 series version 1.3, the protocols used haven't been encrypted as there has been no risk of disclosure of user information.

ABB recommends that customers follow the steps outlined in the section "Mitigating Factors".

Based on the customers risk assessment and exposure of the system, the maintenance release could be applied.

Customers shall contact their local ABB contacts to obtain the maintenance release.

Vulnerability Details

Affected products generate predictable TCP Initial Sequence Numbers which may allow an attacker to predict the correct TCP ISN and used to spoof or disrupt TCP connections of the affected products.

Mitigating Factors

Recommended security practices and firewall configurations can help protect a substation automation network from attacks that originate from outside the network.

Such practices include that substation automation systems are physically protected from direct access by unauthorized personnel, have no direct connections to the Internet, and

ABB Doc Id: 1MRG023796	Date 2016-10-24	Lang. English	Rev. A	Page 3/4
---------------------------	--------------------	------------------	-----------	-------------

are separated from other networks by means of a firewall system that has a minimal number of ports exposed, and others that have to be evaluated case by case.

Substation automation systems should not be used for Internet surfing, instant messaging, or receiving e-mails. Portable computers and removable storage media should be carefully scanned for viruses before they are connected to a control system.

Workarounds

Workarounds are described in the *Corrective Action or Resolution* chapter above.

Frequently asked questions

What is the scope of the vulnerability?

An attacker who successfully exploits this vulnerability could spoof or disrupt TCP connections of the affected products.

What causes the vulnerability?

This vulnerability is caused by a weakness in the TCP random number generator algorithm implemented in the operating system (VxWorks) used by the Relion 650 Series.

What is the affected product or component?

In the Relion 650 series, the affected parts are IEC 61850, DNP 3.0 (TCP), FTP/FTPS protocol and the tool access protocol. All protocols uses the TCP stack implemented by the operating system (VxWorks).

What might an attacker use the vulnerability to do?

An attacker who successfully exploits this vulnerability could spoof or disrupt TCP connections of the affected products.

How could an attacker exploit the vulnerability?

An attacker could try to exploit this vulnerability. It would require that the attacker has access to the system network, by connecting to the network either directly or through a wrongly configured or penetrated firewall, or that he installs malicious software on a system node or otherwise infects the network with malicious software. Recommended practices help mitigate such attacks, see section Mitigating Factors above.

Could the vulnerability be exploited remotely?

Yes, an attacker who has network access to an affected system node could exploit this vulnerability. Recommended practices include that substation automation systems are physically protected, have no direct connections to the Internet, and are separated from other networks by means of a firewall system that has a minimal number of ports exposed.



ABB Doc Id:	Date	Lang.	Rev.	Page
1MRG023796	2016-10-24	English	A	4/4

When this security advisory was issued, had this vulnerability been publicly disclosed?

Yes, this vulnerability has been publicly disclosed.

When this security advisory was issued, had ABB received any reports that this vulnerability was being exploited?

No, ABB had not received any information indicating that this vulnerability had been exploited in the 650 Series when this security advisory was originally issued.

Support

For additional information and support please contact your local ABB service organization. For contact information, see www.abb.com/protection-control.

Information about ABB's cyber security program and capabilities can be found at www.abb.com/cybersecurity.